UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MAGISTRATE JUDGE VALDEZ

UNITED STATES OF AMERICA	)	**JUDGE NORGLE**
	)	No. 11 CR 699
v.	)	
	)	Violations: Title 18, United States Code,
YIHAO PU,	)	Sections 1343, 1832(a)(2), 1832(a)(3),
also known as "Ben Pu," and	)	1030(a)(2)(C), and 1519
SAHIL UPPAL	)	
also known as "Sonny Uppal"	)	**SUPERSEDING INDICTMENT**

COUNT ONE

FILED

The SPECIAL JANUARY 2012 GRAND JURY charges:

APR 1 1 2013

1.   At times material:

THOMAS G BRUTON
CLERK, U S DISTRICT COURT

Company A

a.   Company A was located in Red Bank, New Jersey. Its business included the development of high-performance technology and computer source code to support the rapid buying and selling of publicly-traded stocks (commonly referred to as "high frequency trading" or "HFT").

b.   Company A did not make its HFT platform and source code publicly available, nor did it disclose these materials to its investors or customers. These materials constituted confidential business information of Company A and were a significant source of value to Company A.

c.   Company A's employees were instructed and required to keep confidential source code and other information related to Company A's HFT platform. Company A's employees were not permitted to copy, transmit, remove, or

1

otherwise use any part of Company A's HFT platform and source code for non-work related purposes. Company A monitored their employees to ensure that Company A's confidential business information was kept confidential and used only for Company A's business purposes. It was material to Company A that its employees used Company A's confidential business information in a manner consistent with Company A's policies.

Citadel, LLC

d.   Citadel, LLC, was located in Chicago, Illinois, and was a financial firm that operated an HFT platform, which Citadel referred to as Tactical Trading,

e.   Citadel did not make its HFT platform and source code publicly available, nor did it disclose these materials to its investors or customers. These materials constituted confidential business information of Citadel and were a significant source of value to Citadel.

f.   Citadel's employees were instructed and required to keep confidential source code and other information related to Citadel's HFT trading platform. Citadel maintained a company employee handbook, as well as policies on using and protecting Citadel's proprietary and confidential information, which employees were required to review. Among other things, the employee handbook and policies prohibited employees from:

i.   Using or releasing information about any Citadel business to others without proper authorization, whether for business or personal purposes.

ii.   Conducting Citadel business or disclosing information related to Citadel through non-approved electronic communications systems, including email accounts held on third-party email systems not approved by Citadel.

iii.   Removing, copying, transmitting or forwarding any of Citadel's proprietary or confidential information from any location (or permitting anyone else to do so) either electronically or by means of removable media or otherwise, unless specifically authorized by a manager.

iv.   Using a pass code or otherwise encrypting or password protecting any file or online communication without prior authorization.

v.   Downloading software programs or other materials from the internet without prior authorization.

g.   Citadel also required employees to sign a non-disclosure agreement in which Citadel employees agreed to use confidential information only as required to perform their duties for Citadel (and not for their personal benefit or for the benefit of any other individual or entity). The non-disclosure agreement defined confidential information as including information relating to Citadel's internal financial affairs; strategies; portfolio holdings; portfolio management techniques; quantitative analytics and models used to evaluate financial instruments; proprietary software (including the proprietary system architectures); and Citadel's business and investment processes.

3

h. It was material to Citadel that its employees used Citadel's confidential business information in a manner consistent with Citadel's employee handbook, non-disclosure agreement, and policies.

Defendant PU's and Defendant UPPAL's Employment at Company A

i. From on or about July 27, 2009, through on or about March 26, 2010, defendant YIHAO PU, also known as "Ben Pu," was employed by Company A as a Quantitative Analyst. From in or about July 2008, through in or about June 2010, defendant SAHIL UPPAL, also known as "Sonny Uppal," was employed by Company A as a Quantitative Analyst. As Quantitative Analysts, PU's and UPPAL's primary job responsibilities included testing and analyzing HFT strategies.

Defendant PU's Employment at Citadel

j. From in or about May 2010 through on or about August 30, 2011, PU was employed by Citadel as a Quantitative Financial Engineer. As a Quantitative Financial Engineer, PU's primary job responsibilities included working with analysts and researchers to develop and enhance certain of Citadel's HFT strategies.

k. On or about March 25, 2010, PU signed Citadel's non-disclosure agreement.

l. On or about May 17, 2010, on or about his first day of employment at Citadel, PU signed Citadel's Employee Handbook Acknowledgement Form, in which PU acknowledged that he was responsible for reading the employee

handbook, familiarizing himself with its contents, and adhering to all of the policies and procedures of Citadel.

m.   On or about June 15, 2010, and again on or about August 1, 2011, PU certified that he had received Citadel's policies and procedures and understood that he was obligated to comply with them.

Defendant UPPAL's Employment at Citadel

n.   From in or about September 2010 through on or about September 20, 2011, UPPAL was employed by Citadel as a Quantitative Researcher. As a Quantitative Researcher, UPPAL's primary job responsibilities included researching and developing a high-frequency trading strategy for equity investments.

o.   On or about July 30, 2010, UPPAL signed Citadel's non-disclosure agreement.

p.   On or about September 7, 2010, on or about his first day of employment at Citadel, UPPAL signed Citadel's Employee Handbook Acknowledgement Form, in which UPPAL acknowledged that he was responsible for reading the employee handbook, familiarizing himself with its contents, and adhering to all of the policies and procedures of Citadel.

q.   On or about December 1, 2010, and again on or about August 1, 2011, UPPAL certified that he had received Citadel's policies and procedures and understood that he was obligated to comply with them.

2.   From in or about August 2009, through on or about August 30, 2011, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu," and
SAHIL UPPAL, also known as "Sonny Uppal,"

defendants herein, knowingly devised and intended to devise, and participated in, a scheme to defraud Company A and Citadel, and to obtain property by means of materially false and fraudulent pretenses, representations, promises, and the concealment of material facts, as more fully described below.

3.   It was part of the scheme that PU and UPPAL surreptitiously obtained property from Company A and Citadel, namely Company A's and Citadel's confidential business information related to their HFT platforms, by falsely representing that they would abide by Company A's and Citadel's policies, manipulating the computer system of Citadel to take the property without detection, and encrypting certain data to conceal the material fact that they had taken the property. PU and UPPAL misled Company A and Citadel into believing that they had not taken Company A's and Citadel's property, and concealed their scheme from Company A and Citadel by evading systems designed to monitor employee access to and use of their property. The object of the scheme was to use Company A's and Citadel's property and technology for the personal benefit of PU and UPPAL.

4.   It was further part of the scheme that beginning in approximately September 2009, about two months after PU began working for Company A, PU intended, and made plans, to leave Company A. PU sent electronic communications

6

to himself and others related to his plans to start his own trading firm. In particular, on or about January 7, 2010, PU and UPPAL had an electronic communication during which they discussed obtaining more data for trading strategies, and their "non-work related intentions" of starting their own "fund."

5.   It was further part of the scheme that, on or about February 11, 2010, PU falsely represented and promised to a representative of Company A that he would not download and copy Company A's source code to any personal electronic devices. PU did so despite his knowledge that Company A personnel detected that PU had downloaded certain files containing Company A's source code onto his personal computer and further did so after PU was instructed by Company A's Chief Technology Officer to delete the source code from PU's personal computer and to refrain from any further improper downloading and copying of Company A's source code.

6.   It was further part of the scheme that PU, on or about March 25, 2010, signed Citadel's non-disclosure agreement in which he falsely represented and promised that he would use Citadel's confidential business information only as required to perform his duties for Citadel and not for his personal benefit or the benefit of anyone else.

7.   It was further part of the scheme that, on or about March 25, 2010, the same day PU signed Citadel's Non-Disclosure Agreement, PU downloaded and transferred from Company A's secure internal computer servers thousands of files

containing Company A's confidential business information and copied those files onto a personal electronic storage device, namely, a Seagate hard drive. In particular, PU transferred File 1, which contained Company A's HFT strategy and infrastructure source code, and File 2, which contained Company A's source code for computer programs related to Company A's HFT strategy and infrastructure software, from Company A's computer systems to the Seagate hard drive.

8.   It was further part of the scheme that on or about March 26, 2010, PU resigned from Company A and falsely represented to Company A's Chief Technology Officer that PU would not take any Company A source code when he left, when PU knew that he had downloaded and copied Company A's confidential business information, including Files 1 and 2, to a personal electronic storage device the previous day.

9.   It was further part of the scheme that PU, on or about May 17, 2010, signed Citadel Employee Handbook Acknowledgement Forms, in which PU falsely represented and promised that he would adhere to Citadel's policies and procedures and would not without authorization (i) use or release information about Citadel business to others without proper authorization, whether for business or personal purposes; (ii) conduct Citadel business or disclose information related to Citadel through non-approved electronic communications systems, including email accounts held on third-party email systems not approved by Citadel; (iii) remove, copy, transmit or forward any of Citadel's proprietary or confidential information from any

location (or permit anyone else to do so) either electronically or by means of removable media; (iv) use a pass code or otherwise encrypt or password protect any file or online communication without prior authorization; and (v) download software programs or other materials from the internet without prior authorization.

10.   It was further part of the scheme that on or about November 11, 2010, PU circumvented Citadel's computer security measures by creating and configuring two "virtual machines" on his Citadel work computer, in order to surreptitiously download and transmit Citadel's confidential business information to PU's personal electronic storage devices via computer ports that had been disabled by Citadel. PU concealed the download and transfer from Citadel by encrypting data and failing to disclose to Citadel that he had manipulated its computer systems and taken its property without authorization as required.

11.   It was further part of the scheme that on or about December 29, 2010, PU emailed market data, which was confidential business information of Citadel, to PU's personal email account, which account was held on a third-party email system not approved by Citadel.

12.   It was further part of the scheme that on at least 11 occasions, beginning on or about July 18, 2011, through on or about August 22, 2011, PU, by using the virtual machines, connected personal electronic storage devices to ports on his Citadel work computer and downloaded, copied, and transmitted confidential business information of Citadel to those devices. In particular, between on or about

August 3, 2011, and on or about August 26, 2011, PU downloaded and transmitted File 3, File 4, File 5, and File 6 from a Citadel computer server to a personal electronic storage device.

13.   It was further part of the scheme that, from on or about July 20, 2011, through on or about August 2, 2011, PU and UPPAL accessed their personal email accounts using Citadel computer system to discuss UPPAL's removal of proprietary code from Citadel.

14.   It was further part of the scheme that on or about July 20, 2011, UPPAL transferred confidential business information of Citadel, namely, proprietary Citadel software code for evaluating data and building testing models, from Citadel's secure computer system to PU's personal computer system, when PU and UPPAL knew that such transfer was not authorized by Citadel.

15.   It was further part of the scheme that on or about July 26, 2011, UPPAL transferred from UPPAL's Citadel work computer confidential business information of Citadel, namely, File 7, File 8, and File 9 to an "R session" (a method by which multiple people can simultaneously use a computer program written in the R computer language), which was conducted jointly by PU and UPPAL.

16.   It was further part of the scheme that on or about August 1, 2011, PU and UPPAL certified and acknowledged that they had received Citadel's policies and procedures and were obligated to comply with them, when PU and UPPAL knew that

days earlier UPPAL had, without authorization and against Citadel's policies and procedures, transferred File 7, File 8, and File 9 to their joint R session.

17.   It was further part of the scheme that on or about August 26, 2011, when Citadel representatives confronted PU and asked him about the virtual machines and whether he had plugged any unauthorized device into his Citadel work computer, PU falsely represented that he had only downloaded non-confidential information to his cellular telephone.

18.   It was further part of the scheme that on or about August 26, 2011, after Citadel confronted PU about the virtual machines and his downloading and transmitting of Citadel's confidential business information, PU and UPPAL, with the assistance of Individual A, concealed from Citadel the existence of a number of pieces of computer equipment, including a Hitachi hard drive belonging to PU and the Seagate hard drive that contained Citadel's confidential business information, by removing the computer equipment from PU's apartment and giving the computer equipment to Individual A.

19.   It was further part of the scheme that PU caused Individual A to dispose of certain computer equipment, including the Hitachi hard drive, at or near a sanitary canal near Wilmette Harbor, Illinois.

20.   It was further part of the scheme that on or about August 30, 2011, during an interview with Citadel representatives, UPPAL concealed from Citadel

that he assisted PU in removing from PU's apartment computer equipment that contained confidential business information of Citadel.

21.   It was further part of the scheme that PU and UPPAL concealed, misrepresented, and hid and caused to be concealed, misrepresented, and hidden, the existence and purpose of the scheme and the acts done in furtherance of the scheme.

22.   On or about November 11, 2010, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu,"

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely the downloading onto PU's Citadel work computer in Chicago, Illinois, of the software program, "utorrent.exe," from utorrent's website, whose computer servers were located outside the State of Illinois, to facilitate the creation and configuration of virtual machines on PU's Citadel work computer;

In violation of Title 18, United States Code, Section 1343.

COUNT TWO

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about November 11, 2010, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu,"

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely the downloading of Ubuntu Linux torrent files from Ubuntu Linux's website, whose computer servers were located outside the State of Illinois, to PU's Citadel work computer in Chicago, Illinois, to facilitate the creation and configuration of unauthorized virtual machines on PU's Citadel work computer;

In violation of Title 18, United States Code, Section 1343.

COUNT THREE

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about December 29, 2010, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu,"

defendant herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely an email containing market data that was confidential business information of Citadel, sent using PU's Citadel work computer in Chicago, Illinois, to PU's personal email account at Cornell University in Ithaca, New York;

In violation of Title 18, United States Code, Section 1343.

14

COUNT FOUR

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about July 22, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

<div style="text-align:center">

YIHAO PU, also known as "Ben Pu," and
SAHIL UPPAL, also known as "Sonny Uppal,"

</div>

defendants herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely a GMail instant message session, or "Gchat," between PU and UPPAL, which was routed through Google's computer servers located outside the State of Illinois, in which PU and UPPAL discussed their need for a larger amount of market data to test code for their use in trading strategies that were not authorized by Citadel;

In violation of Title 18, United States Code, Section 1343.

COUNT FIVE

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about July 25, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu," and
SAHIL UPPAL, also known as "Sonny Uppal,"

defendants herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely a GMail instant message session, or "Gchat," between PU and UPPAL, which was routed through Google's computer servers located outside the State of Illinois, in which PU and UPPAL discussed their need for a system to profitably trade the market;

In violation of Title 18, United States Code, Section 1343.

16

COUNT SIX

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about July 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

<div align="center">

YIHAO PU, also known as "Ben Pu," and
SAHIL UPPAL, also known as "Sonny Uppal,"

</div>

defendants herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely a GMail instant message session, or "Gchat," between PU and UPPAL, which was routed through Google's computer servers located outside the State of Illinois, in which PU and UPPAL discussed their joint R session;

In violation of Title 18, United States Code, Section 1343.

COUNT SEVEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about July 29, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

> YIHAO PU, also known as "Ben Pu," and
> SAHIL UPPAL, also known as "Sonny Uppal,"

defendants herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely a GMail instant message session, or "Gchat," between PU and UPPAL, which was routed through Google's computer servers located outside the State of Illinois, in which PU and UPPAL discussed obtaining years' worth of market or "tick" data;

In violation of Title 18, United States Code, Section 1343.

COUNT EIGHT

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about August 7, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu," and
SAHIL UPPAL, also known as "Sonny Uppal,"

defendants herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely an electronic trading order for an E-Mini S&P 500 futures contract, sent from Chicago, Illinois, through PU's Interactive Brokers account, whose computer servers were located in Greenwich, Connecticut;

In violation of Title 18, United States Code, Section 1343.

19

COUNT NINE

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 through 21 of Count One of this superseding indictment are incorporated here.

2.   On or about August 10, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu," and
SAHIL UPPAL, also known as "Sonny Uppal,"

defendants herein, for the purpose of executing the above-described scheme, knowingly caused to be transmitted by means of wire communication in interstate commerce certain writings, signs, and signals, namely an electronic trading order for E-Mini S&P 500 futures contract sent from Chicago, Illinois, through PU's Interactive Brokers account, whose computer servers were located in Greenwich, Connecticut;

In violation of Title 18, United States Code, Section 1343.

COUNT TEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraph 1(a)-(c) of Count One of this superseding indictment are incorporated here.

2.   At times material:

Company A's Trade Secrets

a.   Company A used its HFT platform to trade securities on national exchanges. Company A also developed "infrastructure" software that enabled customers to execute their own HFT trades using Company A's technology. Company A licensed its HFT infrastructure software to national customers through a subsidiary.

b.   Company A's HFT platform included automated trading strategies that identified short-term investment opportunities in the purchase and sale of United States stocks. These trading strategies were based on mathematical and statistical models of investment instruments and market activities, which were translated into algorithms. Company A incorporated these algorithms into proprietary computer source code for HFT programs that automatically executed trading orders upon the occurrence of certain events in the markets.

c.   Company A's HFT infrastructure software included, among other things, (i) tools that assisted customers in translating their automated trading strategies into computer object code and copying the object code onto Company A's

computer servers in New Jersey, and (ii) tools that assisted customers in communicating with national exchanges regarding trades and setting risk parameters for their trading.

     d.   Company A maintained the source code for its HFT trading strategies and infrastructure on Company A's servers located in New Jersey and Illinois. Company A used its HFT trading strategies and platforms to execute securities trades on international financial markets, including the New York Stock Exchange, and further used its HFT trading strategies and platforms to obtain market data from a financial exchange in Chicago, Illinois.

     e.   Company A's HFT strategies and infrastructure software, and their underlying source code, were trade secrets of Company A. In order to protect these trade secrets, Company A took multiple measures to protect their disclosure to unauthorized third persons. These measures included physical security at Company A's offices, limiting and monitoring access to and within Company A's computer networks, instructions to employees regarding the confidentiality of Company A's trading strategy and infrastructure source code, monitoring of employee activity by supervisors, and preventing customers from obtaining access to Company A's source code.

3.   From in or about March 2010, until on or about August 27, 2011, at

Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of

someone other than the owner thereof, knowingly did possess a trade secret

belonging to Company A, namely File 1, which contained Company A's HFT strategy

and infrastructure source code, such trade secret being related to and included in a

product that was produced for and placed in interstate and foreign commerce,

intending and knowing that the offense would injure Company A, and knowing that

the trade secret was stolen and appropriated, obtained, and converted without

authorization;

In violation of Title 18, United States Code, Section 1832(a)(3).

COUNT ELEVEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Ten of this superseding indictment are incorporated here.

2.   From in or about March 2010, until on or about August 27, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly and without authorization did possess a trade secret belonging to Company A, namely File 2, which contained Company A's source code for computer programs related to Company A's HFT strategy and infrastructure software, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Company A, and knowing that the trade secret was stolen and appropriated, obtained, and converted without authorization;

In violation of Title 18, United States Code, Section 1832(a)(3).

COUNT TWELVE

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraph 1(d)-(h), (j)-(m) of Count One of this superseding indictment are incorporated here.

2.   At times material:

Citadel's Trade Secrets

a.   Citadel's Tactical Trading HFT platform deployed automated electronic trading strategies to identify short-term investment opportunities in global equities, futures, and other investment instruments. Citadel's Tactical Trading business used mathematical and statistical computer models to identify and quantify relationships among investment instruments and market activities, and then translated those relationships into algorithms that were incorporated into proprietary computer source code for programs that automatically executed trading orders upon the occurrence of certain events in the markets.

b.   The algorithms incorporated into Citadel's Tactical Trading strategies, commonly referred to by Citadel employees as "alphas," used market data from national and international exchanges and other data (also referred to as "tick data") to predict the movement of investment instruments and other relevant market activity. The output of the alpha algorithms was expressed as numerical values, which Citadel employees referred to as "alpha data" or "alpha values." Furthermore, the alpha algorithms were made up of a series of smaller computations derived from

tick data, referred to as alpha "terms," the output of which was a numerical value referred to as "intermediate" or "term" alpha data.

        c.   Citadel's businesses included receiving investments from outside investors that Citadel used, along with its own money, to make trades based on the predictions generated by its alpha algorithms. Citadel did not make its alpha algorithms, their components, or the output of its algorithms or their components—including source code, alpha data, and term data—publicly available, nor did Citadel disclose these materials to its investors. These materials constituted trade secrets of Citadel and were a significant source of value to Citadel. Investors from throughout the United States placed money with Citadel in part because doing so enabled them to have their funds invested through the use of Citadel's proprietary trading algorithms. Citadel used its proprietary trading algorithms to execute trades on a number of national and international financial markets, including the New York Stock Exchange.

        3.   In order to protect the value of its confidential business information, Citadel took multiple measures to protect its algorithms and their components—including source code, alpha data, and term data—from disclosure to unauthorized third persons. These measures included physical security measures at Citadel's offices; limiting and monitoring access to and within Citadel's computer networks, including the disabling of computer ports; instructions to employees

regarding the handling of proprietary and confidential information; and the monitoring of employee activity.

4.   Between on or about August 9, 2011, and on or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly and without authorization did copy, duplicate, download, upload, replicate, and transmit a trade secret belonging to Citadel, namely, File 3, which contained alpha data and term data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel;

In violation of Title 18, United States Code, Section 1832(a)(2).

COUNT THIRTEEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Twelve of this superseding indictment are incorporated here.

2.   On or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly did possess a trade secret belonging to Citadel, namely, File 3, which contained alpha data and term data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel, and knowing that the trade secret was stolen and, appropriated, obtained, and converted without authorization;

In violation of Title 18, United States Code, Section 1832(a)(3).

COUNT FOURTEEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Twelve of this superseding indictment are incorporated here.

2.   Between on or about August 9, 2011, and on or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly and without authorization did copy, duplicate, download, upload, replicate, and transmit a trade secret belonging to Citadel, namely, File 4, which contained alpha data and term data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel;

In violation of Title 18, United States Code, Section 1832(a)(2).

COUNT FIFTEEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Twelve of this superseding indictment are incorporated here.

2.   On or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly did possess a trade secret belonging to Citadel, namely, File 4, which contained alpha data and term data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel, and knowing that the trade secret was stolen and, appropriated, obtained, and converted without authorization;

In violation of Title 18, United States Code, Section 1832(a)(3).

COUNT SIXTEEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Twelve of this superseding indictment are incorporated here.

2.   Between on or about August 3, 2011, and on or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly and without authorization did copy, duplicate, download, upload, replicate, and transmit a trade secret belonging to Citadel, namely, File 5, which contained alpha data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel;

In violation of Title 18, United States Code, Section 1832(a)(2).

COUNT SEVENTEEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Twelve of this superseding indictment are incorporated here.

2.   On or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly did possess one or more trade secrets belonging to Citadel, namely, File 5, which contained alpha data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel, and knowing that the trade secret was stolen and appropriated, obtained, and converted without authorization;

In violation of Title 18, United States Code, Section 1832(a)(3).

COUNT EIGHTEEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Twelve of this superseding indictment are incorporated here.

2.   Between on or about August 3, 2011, and on or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly and without authorization did, and attempted to, copy, duplicate, download, upload, replicate, and transmit a trade secret belonging to Citadel, namely, File 6, which contained alpha data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel;

In violation of Title 18, United States Code, Section 1832(a)(2).

COUNT NINETEEN

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2 of Count Twelve of this superseding indictment are incorporated here.

2.   On or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, with intent to convert a trade secret to the economic benefit of someone other than the owner thereof, knowingly did possess a trade secret belonging to Citadel, namely, File 6, which contained alpha data, such trade secret being related to and included in a product that was produced for and placed in interstate and foreign commerce, intending and knowing that the offense would injure Citadel, and knowing that the trade secret was stolen and appropriated, obtained, and converted without authorization;

In violation of Title 18, United States Code, Section 1832(a)(3).

COUNT TWENTY

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraph 1(d)-(h), (j)-(m) of Count One of this superseding indictment are incorporated here.

2.   At times material:

a.   Citadel maintained a EMC CELERRA VG8 server with serial number APM00104100381 on which it stored information related to its businesses.

b.   The EMC CELERRA VG8 server with serial number APM00104 100381 was used in and affecting interstate commerce.

c.   Because of PU's position at Citadel, Citadel granted PU access to certain alpha data and term data. PU did not have permission to download or transfer alpha data and term data from Citadel's computer systems to removable storage devices or to use alpha data or term data for non-work related purposes.

3.   Between on or about August 9, 2011, and on or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, intentionally accessed a computer, namely a EMC CELERRA VG8 server with serial number APM00104100381, without authorization and exceeding authorized access, and thereby obtained information, namely File 3 and File 4, which contained alpha data and term data, from a protected computer that was used in and affecting interstate commerce;

In violation of Title 18, United States Code, Sections 1030(a)(2)(C).

COUNT TWENTY-ONE

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraphs 1 and 2(c) of Count Twenty of this superseding indictment are incorporated here.

2.   At times material:

a.   Citadel permitted defendant PU to use a Dell Precision computer with serial number 3F379F1 as his work computer.

b.   The Dell Precision computer with serial number 3F379F1 was used in and affecting interstate commerce.

3.   Between on or about August 3, 2011, and on or about August 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

YIHAO PU, also known as "Ben Pu,"

defendant herein, intentionally accessed a computer, namely a Dell Precision computer with serial number 3F379F1, without authorization and exceeding authorized access, and thereby obtained information, namely File 5 and File 6, which contained alpha data, from a protected computer that was used in and affecting interstate commerce;

In violation of Title 18, United States Code, Section 1030(a)(2)(C).

COUNT TWENTY-TWO

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraph 1(d)-(h), (j)-(q) of Count One of this superseding indictment are incorporated here.

2.   At times material:

a.   Citadel maintained a EMC CELERRA VG8 server with serial number APM00103903310 on which it stored information related to its businesses.

b.   The EMC CELERRA VG8 server with serial number APM0010 3903310 was used in and affecting interstate commerce.

c.   Because of UPPAL's position at Citadel, UPPAL created, and Citadel granted UPPAL access to, File 7, File 8, and File 9, which were designed to optimize a trading strategy by testing the efficacy of that trading strategy under a range of market conditions. More specifically, the research programs were written to: (i) load a fully specified trading strategy, which would contain the alphas, alpha data, market parameters and historical market data; and (ii) map out information about the results of the trading strategy, including its profitability, so that those results could be analyzed. Citadel did not authorize PU to access or obtain File 7, File 8, or File 9, and Citadel did not authorize UPPAL to transfer File 7, File 8, or File 9 to PU.

3.   On or about July 26, 2011, at Chicago, in the Northern District of Illinois, Eastern Division,

<div style="text-align: center">YIHAO PU, also known as "Ben Pu,"</div>

defendant herein, intentionally accessed a computer, namely a EMC CELERRA VG8 server with serial number APM00103903310, without authorization and exceeding authorized access, and thereby obtained information, namely File 7, File 8 and File 9, from a protected computer that was used in and affecting interstate commerce;

In violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 2.

COUNT TWENTY-THREE

The SPECIAL JANUARY 2012 GRAND JURY further charges:

1.   The allegations in Paragraph 1 of Count One of this superseding indictment are incorporated here.

2.   From on or about March 25, 2010, to on or about August 22, 2011, PU and UPPAL obtained confidential business information from Company A and Citadel, including Files 1 through 8. PU used two "virtual machines" on his Citadel work computer to download some of Citadel's confidential business information, and stored information belonging to Company A and Citadel on a Seagate computer hard drive and a Hitachi computer hard drive.

3.   On or about August 26, 2011, Citadel representatives confronted PU concerning the unauthorized virtual machines on his Citadel work computer. Citadel representatives instructed PU to return to Citadel, and preserve and not destroy, any of Citadel's confidential information in his possession. PU was further instructed to refrain from deleting, overwriting, altering, and modifying any documents, records, and electronic files relating or referring to Citadel.

4.   On or about August 26, 2011, PU and UPPAL, acting with the belief that a federal investigation into PU's and UPPAL's conduct might begin at some point in the future, with the assistance of Individual A, concealed and transferred from PU's apartment to Individual A's apartment computer equipment, including

PU's personal Seagate computer hard drive, which contained File 1 and File 2, and PU's personal Hitachi hard drive, which contained File 5 and File 6.

5.   On or about August 28, 2011, at or near a sanitary canal near Wilmette Harbor, Illinois, PU caused Individual A to dispose of certain computer equipment, including the Hitachi hard drive.

6.   From on or about August 26, 2011, to on or about August 28, 2011, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere,

YIHAO PU, also known as "Ben Pu," and
SAHIL UPPAL, also known as "Sonny Uppal,"

defendants herein, together with Individual A, knowingly altered, destroyed, concealed, and covered up a record, document and tangible object, namely computer equipment that contained electronic documents and files containing proprietary and confidential information of Company A and Citadel, with the intent to impede, obstruct, and influence the investigation and proper administration of any matter within the jurisdiction of any department and agency of the United States, and in relation to and contemplation of any such matter and case;

In violation of Title 18, United States Code, Section 1519.

FORFEITURE ALLEGATION ONE

The SPECIAL JANUARY 2012 GRAND JURY further alleges:

1.　　The allegations of Counts Ten through Nineteen of this superseding indictment are incorporated here for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 1834.

2.　　As a result of his violations of Title 18, United States Code, Section 1832(a), as alleged in the superseding indictment,

YIHAO PU, also known as "Ben Pu,"

defendant herein, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1834, (i) any and all property constituting, and derived from, any proceeds the defendant obtained, directly and indirectly, as a result of the violations; and (ii) any and all property used, and intended to be used, in any manner or part, to commit and facilitate the commission of the violations, including the following:

　　　　a.　　Western Digital Hard Drive, Serial Number WX61E41FC897;

　　　　b.　　Seagate Hard Drive, Serial Number 9XW00KFP;

　　　　c.　　Hitachi Hard Drive, Serial Number MH3R4VAK;

　　　　d.　　Motorola Droid phone, Serial Number 268435458113866000;

　　　　e.　　Lenovo X300 computer, Serial Number L3A7192;

3.   If any of the property described above as being subject to forfeiture pursuant to Title 18, United States Code, Section 1834, as a result of any act or omission of the defendant:

(a)   cannot be located upon the exercise of due diligence;

(b)   has been transferred or sold to, or deposited with, a third party;

(c)   has been placed beyond the jurisdiction of the court;

(d)   has been substantially diminished in value; or

(e)   has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property under the provisions of Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1834,

All pursuant to Title 18, United States Code, Section 1834.

FORFEITURE ALLEGATION TWO

The SPECIAL JANUARY 2012 GRAND JURY further alleges:

1.   The allegations of Counts Twenty through Twenty-Two of this superseding indictment are incorporated here for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 1030(i)-(j).

2.   As a result of his violations of Title 18, United States Code, Section 1030(a), as alleged in the superseding indictment,

YIHAO PU, also known as "Ben Pu,"

defendant herein, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i)-(j): (i) his interest in any personal property that was used and intended to be used to commit and to facilitate the commission of such violation; and (ii) any property, real and personal, constituting and derived from, any proceeds that defendant obtained, directly and indirectly, as a result of such violations, including the following:

      a.   Western Digital Hard Drive, Serial Number WX61E41FC897;

      b.   Seagate Hard Drive, Serial Number 9XW00KFP;

      c.   Hitachi Hard Drive, Serial Number MH3R4VAK;

      d.   Motorola Droid phone, Serial Number 268435458113866000;

      e.   Lenovo X300 computer, Serial Number L3A7192;

3.   If any of the property described above in Paragraph 2 as being subject to forfeiture pursuant to Title 18, United States Code, Section 1030(i)(1)(B), as a result of any act or omission of the defendant:

(a)   cannot be located upon the exercise of due diligence;

(b)   has been transferred or sold to, or deposited with, a third party;

(c)   has been placed beyond the jurisdiction of the court;

(d)   has been substantially diminished in value; or

(e)   has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property under the provisions of Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2) and Title 18, United States Code, Section 982(b)(1),

All pursuant to Title 18, United States Code, Section 1030(i)-(j).

A TRUE BILL:

_____

FOREPERSON

_____

UNITED STATES ATTORNEY

45